Exhibit A1

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

LUCISBEL CRUZ-BERMUDEZ and HELMUT BECKER, on behalf of themselves and all others similarly situated, Plaintiffs, v. **HENRY SCHEIN, INC.**, Defendant.	Case No.: 2:24-cv-00387-JMW **FIRST AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Lucisbel Cruz-Bermudez and Helmut Becker ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this First Amended Class Action Complaint against Defendant Henry Schein, Inc. ("Henry Schein" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, their counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant Henry Schein (Nasdaq: HSIC) is an international distributor of health care products and services.[1] And in 2022, Defendant boasted $12.6 billion in revenue.[2]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its

[1] *About Us*, HENRY SCHEIN, https://investor.henryschein.com/aboutus?hsi_domain=www.henryschein.com&hsi_locale=us-en (last visited Jan. 16, 2024).
[2] *Id*.

current and former customers, employees, and employees' dependents. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the PII/PHI of its current and former customers, employees, and employees' dependents.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs are Data Breach victim, having received a breach notice. They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, the private information of current and former customers, employees, and employees' dependents was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Lucisbel Cruz-Bermudez, is natural person and citizen of South Carolina. She resides in Anderson, South Carolina where she intends to remain.

9. Plaintiff Helmut Becker is a natural person and citizen of Germany. He resides in Frankfurt am Main, Germany, where he intends to remain.

10. Defendant, Henry Schein, Inc., is a Foreign Business Corporation incorporated in Delaware and with its principal place of business at 135 Duryea Road, Melville, New York 11747.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff Cruz-Bermudez and Defendant are citizens of different states. And there are over 100 putative Class members.

12. This Court has personal jurisdiction over Defendant because it is headquartered in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York.

13. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiffs and the Class

14. Defendant Henry Schein (Nasdaq: HSIC) is an international distributor of health care products and services.[3] And in 2022, Defendant boasted $12.6 billion in revenue.[4]

[3] *About Us*, HENRY SCHEIN, https://investor.henryschein.com/aboutus?hsi_domain=www.henryschein.com&hsi_locale=us-en (last visited Jan. 16, 2024).
[4] *Id*.

15. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former customers, employees, and employees' dependents.

16. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their PII/PHI.

17. Under state and federal law, businesses like Defendant have duties to protect the PII/PHI of its current and former customers, employees, and employees' dependents and to notify them about breaches.

18. Defendant recognizes these duties, declaring in its "Privacy Statement" that:

a. "At Henry Schein, Inc., your privacy is important to us."[5]

b. "We process personal information in different contexts, and we do so by respecting your privacy, as part of our unwavering commitment to ethical and responsible practices and as required by law."[6]

c. "This Privacy Statement ('Statement') sets forth the principles that govern our treatment of personal information across Henry Schein, Inc. and its controlled subsidiaries and affiliates operating in the United States ('Henry Schein'). All employees and those with whom we share personal information must adhere to this Statement."[7]

[5] *Privacy Statement*, HENRY SCHEIN, https://www.henryschein.com/us-en/Privacy.aspx?PageType=popup (last visited Jan. 16, 2024).
[6] *Id.*
[7] *Id.*

d. "Henry Schein is committed to protecting personal information that our employees, customers, prospects, suppliers, and vendors have entrusted to us."[8]

e. "We collect and use personal information in order to perform our business functions and provide quality health care products and services to our customers."[9]

f. "This Statement applies to personal information in any format or medium, relating to employees, customers, vendors and others who do business with Henry Schein."[10]

g. "We recognize personal information as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household."[11]

h. "Our record retention schedule prescribes maximum retention periods of information for business, legal, or operational requirements. Generally, data . . . is retained between 6 and 10 years or as otherwise stated below."[12]

i. Notably, Defendant declares that the "maximum retention period[]" is "10 years" for "[p]ersonal information categories" including "[a] name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education,

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."[13]

j. Similarly, Defendant declares that "maximum retention period[]" is "7 years" for "[p]rofessional or employment related information."[14]

k. "We apply the data minimization principle in the collection and use of personal information with the aim to only collect information that is necessary and by fair means and providing notice and requiring consent when necessary."[15]

l. "The use of personal information for new purposes should be consistent with and meet privacy expectations described in this Statement, otherwise we will request your authorization."[16]

m. "Henry Schein is committed to security, confidentiality, and integrity of personal information in accordance with legal requirements."[17]

n. "We take commercially reasonable precautions to keep personal information secure against unauthorized access and use and we periodically review our security measures."[18]

o. "We are committed to processing your data in a secure manner and have put in place specific technical and organizational measures to prevent the

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*

personal information we hold from being accidentally or deliberately compromised."[19]

p. "Our employees participate in a training and compliance program and are required to safeguard your information."[20]

q. "If you reside or otherwise find yourself in jurisdictions with data protection laws, Henry Schein is committed to supporting your rights granted by such applicable data protection laws."[21]

19. Likewise, via its "Recruitment Privacy Statement," Defendant represents that:

a. "This Recruitment Privacy Statement ("Privacy Statement") describes how Henry Schein collects, uses, discloses, transfers, and stores personal data as part of our recruitment process for companies in the Henry Schein group."[22]

b. "We only disclose your personal data to those who require access to perform their tasks and duties, and to third parties that have a legitimate purpose for accessing it."[23]

c. "We will implement appropriate measures to provide assurance that other Henry Schein subsidiaries or third-party organizations that we use to process data on our behalf use information in a manner consistent with this

---

[19] *Id*.
[20] *Id*.
[21] *Id*.
[22] *Recruitment Privacy Statement*, HENRY SCHEIN (Dec. 17, 2021) https://www.henryschein.com/us-en/images/career/Recruitment-Privacy-Statement-12.30.2021-Updated.pdf.
[23] *Id*.

Privacy Statement and with applicable law, and that the security and confidentiality of the information is maintained."[24]

d. "Third-party organizations processing personal data for Henry Schein must comply with all relevant privacy laws in order to protect your personal data in any country where they process or transfer the data."[25]

e. "Your personal data will be stored in accordance with applicable laws and kept as long as needed to carry out the purposes described in this Privacy Statement or as otherwise required by applicable law."[26]

f. "Henry Schein operates as a global business and may transfer, store, or process your personal data in a country outside your jurisdiction, including countries outside the European Union/European Economic Area ('EU/EEA') or Switzerland. However, we have taken appropriate safeguards with respect to the protection of your privacy, fundamental rights and freedoms, and the exercise of your rights. For example, if we transfer personal data from the EU/EEA or Switzerland to a country outside it, such as the United States, we will implement an appropriate data transfer solution, such as entering into EU Standard Contractual Clauses with the data importer or taking other measures to provide an adequate level of data protection under EU law."[27]

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*

g. "We use technical and organizational measures that provide a level of security appropriate to the risk of processing your personal data."[28]

Defendant's Data Breach

20. On September 27, 2023, Defendant was hacked.[29] And because of this Data Breach, Plaintiffs' and Class Members' PII/PHI were "accessed and obtained by an unauthorized third party."[30]

21. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. addresses;

c. phone numbers;

d. email addresses;

e. photographs;

f. dates of birth;

g. demographic information;

h. background information;

i. government-issued identification numbers;

j. Social Security numbers;

k. driver's license numbers;

l. state identification numbers;

---

[28] *Id*.
[29] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/6a08eecd-1ccf-451e-a419-a0b873114853.shtml (last visited Jan. 16, 2024).
[30] *Id*.

m. passport numbers;

n. financial information;

o. bank account information;

p. credit card numbers;

q. loan information;

r. medical history;

s. medical treatment;

t. insurance information;

u. employment information (e.g., job title, compensation);

v. IP address.[31]

22. Moreover, Defendant admitted that the Data Breach also exposed "other information."[32] Thus, upon information and belief, the Data Breach exposed a broader range of PII/PHI than listed herein.

23. Additionally, Defendant admitted that the Data Breach exposed the "personal information . . . about an employee's dependents."[33]

24. In total, Defendant injured at least 29,112 persons—via the exposure of their PII/PHI—in the Data Breach.[34] Upon information and belief, these 29,112 persons include its current and former customers, employees, and employees' dependents.

---

[31] *Notice of Data Breach*, CAL. ATTY GEN, https://oag.ca.gov/ecrime/databreach/reports/sb24-577534 (last visited Jan. 16, 2024).
[32] *Id*.
[33] *Id*.
[34] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/6a08eecd-1ccf-451e-a419-a0b873114853.shtml (last visited Jan. 16, 2024).

25. And yet, Defendant waited over until November 17, 2023, before it began notifying the class—a full 51 days after the Data Breach began.[35]

26. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

27. Moreover, Defendant has been less than forthcoming about the precise dates regarding (1) the start of the Data Breach, and (2) when Defendant discovered its own Data Breach. Thus, upon information and belief, the Data Breach began prior to September 27, 2023.

28. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "remain vigilant by reviewing account statements and monitoring free credit reports;"

b. "[w]e recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies;"

c. "we recommend that you regularly review the explanation of benefits statements that you receive from your insurer;"

d. "order copies of your credit reports and check for any medical bills that you do not recognize;" and

[35] *Id.*

e. "educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission."[36]

29. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

30. Since the breach, Defendant has promised to be "seeking to implement measures to fortify our defenses going forward."[37] But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

31. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

32. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

33. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Defendant inflicted upon them.

---

[36] *Notice of Data Breach*, CAL. ATTY GEN, https://oag.ca.gov/ecrime/databreach/reports/sb24-577534 (last visited Jan. 16, 2024).
[37] *Id.*

34. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiffs and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class members.

35. Worse yet, this Data Breach reflects a *pattern* of negligent data security by Defendant. After all, Defendant already admitted—in its discloses to the Maine Attorney General—that *just within the past 12 months*, Defendant (and/or Defendant's subsidiaries) experienced data breaches on the following dates:

a. December 19, 2022;

b. March 31, 2023; and

c. June 01, 2023.[38]

36. Worryingly, the cybercriminals that obtained Plaintiffs' and Class members' PII/PHI appear to be the notorious cybercriminal group "BlackCat/ALPHV."[39] Specifically, reports reveal that:

a. "The BlackCat ransomware gang added Henry Schein to its dark web leak site, saying it breached the company's network and allegedly stole 35 terabytes of sensitive data."[40]

b. "According to the cybercrime operation, they re-encrypted the company's devices after negotiations faltered towards the end of October while Henry Schein was on the verge of restoring its systems."[41]

---

[38] *Id*.
[39] Sergiu Gatlan, *Healthcare giant Henry Schein hit twice by BlackCat ransomware*, BLEEPING COMPUTER (Nov. 27, 2023) https://www.bleepingcomputer.com/news/security/healthcare-giant-henry-schein-hit-twice-by-blackcat-ransomware/.
[40] *Id*.
[41] *Id*.

c. "This would make this month's incident the third time since October 15 that BlackCat encrypted Henry Schein's systems after breaching its network."[42]

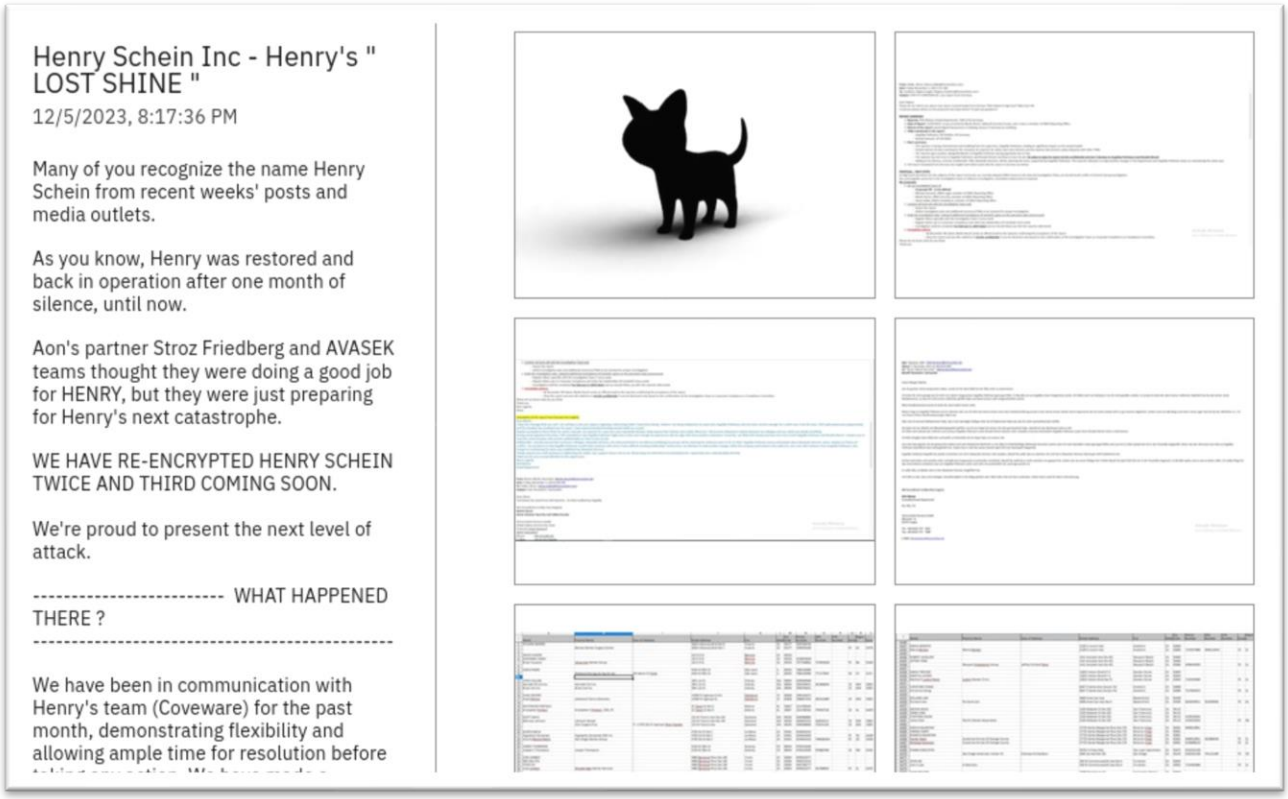
37. Worse yet, BlackCat/ALPHV appears to be actively *publishing* the stolen PII/PHI on the Dark Web. Specifically, BlackCat/ALPHV declared that:

a. "As of midnight today, a portion of their internal payroll data and shareholder folders will be published on our collections blog."[43]

b. "We will continue to release more data daily."[44]

38. Furthermore, a screenshot of BlackCat/ALPHV's Dark Web website seemingly confirms that the cybercriminals are actively *publishing* the stolen PII/PHI.[45]

[42] *Id*.
[43] *Id*.
[44] *Id*.
[45] *See Henry Schein Inc*., RANSOM LOOK, https://www.ransomlook.io/screenshots/alphv/Henry%20Schein%20Inc%20-%20Henry%27s%20%22%20LOST%20SHINE%20%22.png (last visited Jan. 17, 2023).



39. ALPHV Blackcat is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about ALPHV Blackcat.[46] Specifically, the joint "Cybersecurity Advisory" (CSA) stated, *inter alia*, that:

a. "ALPHV Blackcat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide targeted via ransomware and/or data extortion."[47]

b. "This ALPHV Blackcat update has the capability to encrypt both Windows and Linux devices, and VMWare instances."[48]

---

[46] *ALPHV Blackcat*, FBI & CISA (Dec. 19, 2023) https://www.cisa.gov/sites/default/files/2023-12/aa23-353a-stopransomware-alphv-blackcat_0.pdf.
[47] *Id.*
[48] *Id.*

c. "ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations."[49]

d. "According to the FBI, as of September 2023, ALPHV Blackcat affiliates have compromised over 1000 entities—nearly 75 percent of which are in the United States and approximately 250 outside the United States—, demanded over $500 million, and received nearly $300 million in ransom payments."[50]

e. "ALPHV Blackcat affiliates use advanced social engineering techniques and open source research on a company to gain initial access."[51]

f. "Some ALPHV Blackcat affiliates exfiltrate data after gaining access and extort victims without deploying ransomware. After exfiltrating and/or encrypting data, ALPHV Blackcat affiliates communicate with victims via TOR, Tox, email, or encrypted applications."[52]

40. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[53]

41. Thus, on information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

PLAINTIFFS' EXPERIENCES

---

[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

Plaintiff Cruz-Bermudez's Experience

42. Plaintiff Lucisbel Cruz-Bermudez is a former employee of Defendant—having worked for Defendant from approximately March 2015 until November 2018.

43. Thus, Defendant obtained and maintained Plaintiff's PII/PHI.

44. As a result, Plaintiff was injured by Defendant's Data Breach.

45. As a condition of her employment with Defendant, Plaintiff provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

46. Plaintiff provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

47. Plaintiff reasonably understood that a portion of the funds paid to Defendant (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of PII/PHI.

48. Plaintiff received a Notice of Data Breach on January 16, 2024—attached as Exhibit A.

49. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

50. Through its Data Breach, Defendant compromised Plaintiff's:

a. name;

b. addresses;

c. phone numbers;

d. email addresses;

e. photographs;

f. date of birth;

g. demographic information;

h. background information;

i. government-issued identification numbers;

j. Social Security number;

k. driver's license number;

l. state identification number;

m. passport number;

n. financial information;

o. bank account information;

p. credit card numbers;

q. loan information;

r. medical history;

s. medical treatment;

t. insurance information;

u. employment information (e.g., job title, compensation);

v. IP address; and

w. other information.

51. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

52. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam emails, text messages and phone calls.

53. Such injuries are traceable to Defendant's Data Breach, because Defendant's notice to Plaintiff indicated that her (1) email addresses, and (2) phone numbers were exposed.

54. Broadly speaking, Plaintiff has suffered from the following spam and/or scam texts, calls, and emails about: (1) medical insurance, (2) Medicaid, (3) Medicare, (4) auto insurance, and (5) bank accounts.

55. For example, Plaintiff suffered from, *inter alia*, the following specific spam and/or scams:

a. Plaintiff received a scam call whereby the caller masqueraded itself as being from "Bank of America." The scammer told Plaintiff that the call was to discuss "suspicious activity" on her account. Plaintiff has an account with Bank of America, and thus, the scammer deceived her into believing that she was talking to her bank—as such, Plaintiff gave the scammer both her name and date of birth.

b. Plaintiff received scams regarding Medicaid—which Plaintiff uses. As such, Plaintiff was deceived by these scammers because she does indeed use Medicaid.

c. Plaintiff received a scam call which (1) identified Plaintiff by name (Lucisbel Cruz-Bermudez), and (2) identified the precise car that Plaintiff

owns (a Nissan Versa). Thereafter, the scammer began asking various questions about Plaintiff and her vehicle.

56. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

57. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

58. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

59. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

60. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

61. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

62. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Becker's Experience

63. Plaintiff Helmut Becker is a former employee of Defendant—having worked for Defendant from approximately August 2009 through March 2014.

64. Thus, Defendant obtained and maintained Plaintiff's PII/PHI.

65. As a result, Plaintiff was injured by Defendant's Data Breach.

66. As a condition of his employment with Defendant, Plaintiff provided Defendant with his PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

67. Plaintiff provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

68. Plaintiff reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII/PHI.

69. Plaintiff received a Cybersecurity Incident letter, directly from Defendant, informing him that his PII/PHI was impacted in the Data Breach, dated January 31, 2024.

70. Through its Data Breach, Defendant compromised at least the following elements of Plaintiff's PII/PHI:

a. name;

b. addresses;

c. phone numbers;

d. date of birth;

e. title

f. employee ID;

g. date of hire

h. reporting structure

i. MBO achievements.

71. Plaintiff has spent—and will continue to spend—significant time and effort protect himself from identity theft, including changing passwords and resecuring his own computer accounts. After all, Defendant directed Plaintiff to take those steps in its breach notice.

72. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam emails, text messages and phone calls.

73. Such injuries are traceable to Defendant's Data Breach, because Defendant's notice to Plaintiff indicated that his (1) email addresses, and (2) phone numbers were exposed.

74. Broadly speaking, Plaintiff has suffered from the following spam and/or scam texts, calls, and emails about: (1) medical insurance, (2) Medicaid, (3) Medicare, (4) auto insurance, and (5) bank accounts.

75. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

76. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

77. Plaintiff suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

78. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

79. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

80. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

81. Today, Plaintiff has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

82. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

83. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

84. The value of Plaintiffs and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

85. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

86. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

87. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

88. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

89. Defendant disclosed the PII/PHI of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

90. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

91. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

92. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.[54]

93. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[55]

94. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

95. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

96. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[56] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

---

[54] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[55] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[56] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

97. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

98. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

99. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

100. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to the data of its current and former customers, employees, and employees' dependents constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

101. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

102. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

103. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

104. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

105. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[57]

106. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI is properly maintained.[58]

107. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

---

[57] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[58] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

108. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

109. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3),

individually and on behalf of all members of the following class:

> All individuals whose PII/PHI was compromised in the Data Breach discovered by Henry Schein in September 2023, including all those individuals who received notice of the breach.

110. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

111. Plaintiffs reserve the right to amend the class definition.

112. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

113. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

114. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 29,112 members.

115. Typicality. Plaintiffs' claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

116. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs

have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

117. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

118. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

119. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

120. Plaintiffs and the Class (or their third-party agents) entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

121. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

122. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

123. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' PII/PHI.

124. Defendant owed—to Plaintiffs and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

125. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

126. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

127. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

128. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class (or their third-party agents) entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

129. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class members' PII/PHI.

130. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' sensitive PII/PHI.

131. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

132. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class members' PHI.

133. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

134. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

135. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

136. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

137. Defendant breached these duties as evidenced by the Data Breach.

138. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

139. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs and Class members' injury.

140. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class members' injuries-in-fact.

141. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

142. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

143. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

144. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract

(On Behalf of Plaintiffs and the Class)

145. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

146. Plaintiffs and Class members either directly contracted with Defendant or Plaintiffs and Class members were the third-party beneficiaries of contracts with Defendant.

147. Plaintiffs and Class members (or their third-party agents) were required to provide their PII/PHI to Defendant as a condition of receiving products, services, and/or employment provided by Defendant. Plaintiffs and Class members (or their third-party agents) provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's products, services, and/or employment.

148. Plaintiffs and Class members (or their third-party agents) reasonably understood that a portion of the funds they paid to Defendant (and/or funds derived from their employment with Defendant) Defendant would be used to pay for adequate cybersecurity measures.

149. Plaintiffs and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

150. Plaintiffs and the Class members (or their third-party agents) accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for products, services, and/or employment.

151. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

152. In its various privacy policies, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII/PHI.

153. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

154. After all, Plaintiffs and Class members (or their third-party agents) would not have entrusted their PII/PHI to Defendant (or their third-party agents) in the absence of such an agreement with Defendant.

155. Plaintiffs and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

156. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

157. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

158. Defendant materially breached the contracts it entered with Plaintiffs and Class members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

159. In these and other ways, Defendant violated its duty of good faith and fair dealing.

160. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

161. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

162. Plaintiffs and Class members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

164. This claim is pleaded in the alternative to the breach of implied contract claim.

165. Plaintiffs and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII/PHI to provide products, services, and/or facilitate employment.

166. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members (or their third-party agents).

167. Plaintiffs and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were

required to provide based on Defendant's duties under state and federal law and its internal policies.

168. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII/PHI.

169. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

170. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' employment and/or payment because Defendant failed to adequately protect their PII/PHI.

171. Plaintiffs and Class members have no adequate remedy at law.

172. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

173. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

174. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII/PHI; (2) to timely

notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

175. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

176. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

177. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII/PHI.

178. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

179. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FIFTH CAUSE OF ACTION
Violation of the New York Deceptive Trade Practices Act
New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Class)

180. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

181. Under the New York Gen. Bus. Law § 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

182. Notably, Defendant's deceptive acts and/or practices were directed at consumers. After all, via its "Privacy Statement" and "Recruitment Privacy Statement," Defendant represented to consumers that they would, *inter alia*, use reasonably adequate data security.

183. And these deceptive acts—including the quotations provided *supra*—were materially misleading insofar as they induced consumers to rely on such statements and disclose their PII/PHI.

184. Section § 349 applies to Defendant because there is a sufficient nexus between Defendant's conduct and New York. After all, Defendant's corporate headquarters is in the state of New York.

185. And, upon information and belief, the misleading acts and/or practices alleged herein—including the representations in Defendant's "Privacy Statement" and "Recruitment Privacy Statement"—were written, approved, and/or otherwise authorized by Defendant within the state of New York.

186. Defendant violated § 349 by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII/PHI, including

duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII/PHI; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

187. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII/PHI.

188. Defendant intended to mislead Plaintiffs and Class members and induce them to rely on its omissions.

189. Had Defendant disclosed to Plaintiffs and Class members (or their third-party agents) that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII/PHI that Plaintiffs and Class members (or their third-party agents) entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class members acted

reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

190. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class members' rights.

191. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

192. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

193. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

194. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

195. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

196. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs

alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

197. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

198. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

199. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

200. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class members' injuries.

201. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

202. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enters an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: February 16, 2024

Respectfully submitted,

By: /s/ *James J. Bilsborrow*
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
Telephone: (212) 558-5500
JBilsborrow@weitzlux.com

TURKE & STRAUSS LLP
Samuel J. Strauss*
Raina Borrelli*
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Attorneys for Plaintiffs and Proposed Class

**Pro Hac Vice application forthcoming*